Substitute the paragraph starting at page 1, line 25, with the following:

A1 A common example is the software escrow account. Software customers ~~sometime~~ sometimes request that program source code and design documentation be placed into an escrow account for safe keeping. The software customer desires some assurance that the software will survive the demise of the vendor organization (or the departure of key personnel) that developed the software. On the other hand, software source code and design documentation are the crown jewels, the pattern or template from which unlimited quantities of saleable product can be manufactured and vendors typically are very ~~reluctance~~ reluctant to provide copies of this material to their customers.

Substitute the paragraph starting at page 2, line 24, with the following:

A2 Traditional electronic information protection systems are often inflexible and inefficient, and—, further, are vulnerable to unauthorized access. Authorization passwords and protocols, license servers, "lock/unlock" distribution methods, and non-electronic contractual limitations imposed on users are a few of the more prevalent protection schemes. In a business and commercial context, these efforts are inefficient and limited solutions.

Substitute the section heading on page 3, line 5, with the following:

A3 ~~SUMMARY OF THE INVENTION~~ SUMMARY OF THE INVENTION

Substitute the paragraph starting at page 4, line 21, with the following:

A4 The present invention may also be implemented as a method of accessing a secure data storage unit that utilizes the apparatus described above. The method preferably includes initiating a request for access to a dedicated data storage unit, the request specifying the remotely located secure storage facility containing the dedicated data storage unit for which access to is desired and a user identification code designating the desired dedicated data storage unit. In response to the request for access, determining the remote secure storage facility address on a communications network, automatically connecting to the remote secure storage facility, and transmitting the request to the remote secure storage facility. Identifying the dedicated data storage unit associated with the specified user identification code and granting access to the identified dedicated data storage unit in accordance with pre-existing instructions associated with the specified user identification code. The preferred method may also include specifying a processor identification code associated with the client computer and identifying the dedicated data storage unit associated with both the specified user identification code and the specified processor identification code.

Substitute the section heading on page 5, line 12, with the following:

A5 ~~BRIEF DESCRIPTION OF THE DRAWINGS~~ BRIEF DESCRIPTION OF THE DRAWINGS

Substitute the paragraph starting at page 5, line 13, with the following:

A6 The present invention will be described with reference to the accompanying drawings. The components in the drawings ~~are~~ are not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the present invention. In the drawings, like reference numbers indicate identical or functionally similar elements throughout the several views.

Substitute the section heading on page 6, line 1, with the following:

A7 ~~DETAILED DESCRIPTION OF THE INVENTION~~ DETAILED DESCRIPTION OF THE INVENTION

Substitute the paragraph starting at page 11, line 7, with the following:

A8 Alternatively, when submitting an access request, the user would specify only the logical storage device, the "d" drive, for example, and the path elements 44 and 46 without specifying the user ID 42. The logical storage device controller 36 would then ~~attached~~ attach the appropriate user ID to the access request based on the user submitting the access request prior to transmitting the access request to the remote secure storage facility 14, thus making the user ID also transparent to the user. A user would be required to log on to the client computer 12 or to the user application 32 using a secure password, for example, in order for the logical storage device controller 36 to recognize the user submitting ~~a~~ an access request.

Substitute the paragraph starting at page 11, line 17, with the following:

At the remote secure storage facility 14, the system processor 22 identifies ~~(60)the~~ (64) the dedicated data storage unit 20 assigned to the user ID code specified in the access request and grants access to the identified dedicated data storage unit 20 in accordance with a set of instructions (provided by the user and the remote secure storage facility administrator at the time the service is subscribed) for that user ID code. Based on the assigned security level, either the user ID code or both the user ID code and the processor ID code may be required for the system processor 22 to grant access. The set of instructions specify security level for data files stored in the associated dedicated data storage unit 20, whether or not to provide additional encryption of the data file, level of access to be granted, etc. The system processor 22 then encrypts the data file as required with the remote secure storage facility encryption key 24 and stamps (i.e., adds to the file) the data file with the date and time. A filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request. The date/time stamp, reference ID and filename are stored in a database ~~66~~ (66) where a directory for the remote secure storage facility 14 is maintained by the system processor 22. The filename and reference ID is also transmitted (70) back to the client computer 12 via the communications network 16 and stored (72) in a local data base 74 where the logical storage device controller 36 maintains a directory for each of the user-assigned dedicated data storage units.

Substitute the paragraph starting at page 12, line 8, with the following:

Fig. 4 is a flow chart illustrating the process for retrieving a data file from a dedicated data storage unit in a preferred embodiment of the secure data storage system in accordance with the principles of the present invention. A user working (80) in a user application is required to retrieve a data file from secure storage (i.e., an assigned dedicated data storage unit 20). In a manner similar to that described with reference to Fig. 3, to submit an access request, the user simply uses the "open file" command conventionally provided by most user applications. When the list of drives is displayed, the user selects the logical storage device, the "d" drive, for example. This prompts the logical storage device controller 36 to retrieve from the database ~~74~~ (74) and display the directory for the remote secure storage facility 14 indicated by the designator 40 for the logical storage device 36. The user selects (82) the appropriate subdirectory, designated by the user ID code, and the desired data file from the subdirectory. The filename includes the reference ID assigned by the system processor 22 when the data file was stored in the dedicated data storage unit 20 identified by the specified user ID code. When the user has specified the desired data file to be retrieved, the logical storage device controller 36 determines the network address and establishes communications with the remote secure storage facility 14 corresponding to the designator 40 for the logical storage device 34. Prior to transmitting the access request to the remote secure storage facility 14, the controller 36 prompts the user to enter the user name (87) and appends it to the access request. The controller 36 then transmits the access request to the remote secure storage facility 14 via the communications network 16 (86).

Substitute the paragraph starting at page 13, line 1, with the following:

A11 At the remote secure storage facility 14, utilizing the user name, the user ID code and the reference ID, the system processor 22 validates (88) that an authorized user is submitting the access request. If the user is not authorized, the access request is denied (90) and a message is sent to client computer 12 cross-referenced to the reference ID specified in the access request and to the owner of the service subscription. Alternatively, in a preferred embodiment, the validation process may be performed by human administrators rather than by the system processor 22; for example, a telephone call to a previously authorized phone number to validate the request. If the access request is valid (i.e., submitted by an authorized user) the system processor 22 grants access in accordance with the set of instructions associated with the specified user ID code, cross-references the specified reference ID with the filename database 66 and retrieves (92, 68) the desired data file. Using the decryption key 24, the retrieved data file is decrypted removing any encryption provided by the remote secure storage facility at the time the data was stored. The date/time stamp applied to the data file at the time of encryption is used to determine the proper decryption key to be used. The decrypted data file is then transmitted (92) back to the client computer 12 and the user via the communications network 16. If the processor ID was required by the assigned security level when the data file was originally stored, then the receiving computer, the client computer 12, will be prompted for its processor ID ~~100~~ (100) prior to the system processor 22 transmitting the decrypted data file. If the processor ID ~~100~~ (100) is not an authorized processor ID, the data file will not be transmitted and a message is sent to the client computer 12 and the subscription owner. At the receiving computer, the controller 36 decrypts the received data file with the user key to remove any encryption provided at the client computer 12 when

the data file was originally transmitted to the remote secure storage facility 14 for secure storage. Similarly, the logical storage device controller 36 determines that the requesting user is an authorized user for the retrieved file prior to decrypting the data file. When decrypted and authorized, the user can then retrieve (104) the desired file from the logical storage device 34 for the application in use.

A11

Substitute the paragraph starting at page 14, line 4, with the following:

A12

In the several preferred embodiments illustrated above, various functions have been described as being performed by either the logical storage device 34 and its controller 36 or the remote secure storage facility 14 and its system processor 22. It is to be noted that it is not mandatory that all of the described functions be assigned to the particular components as described above, but that many of these functions can be performed by either the logical storage device 34 and ~~it~~ its controller 36 or the remote secure storage facility 14 and its system processor 22. For example, functions such as creating and deleting data files, writing to and reading from the data files can be performed by either the logical storage device controller 36 or the remote secure storage facility system processor 22. Similarly, the directory for the remote secure storage facility 14 may be maintained at the remote secure storage facility only and transmitted to a user for display at each instance an access request has been received and access to the specified dedicated data storage unit 20 has been granted.

Substitute the paragraph starting at page 15, line 8, with the following:

A13 Also, the flow charts of Figs. 3 and 4 show the architecture, functionality, and operation of a possible implementation of the logic. In this regard, each block represents a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that in some alternative implementations, the functions noted in the blocks may occur out of the order noted in Figs. 3 and 4. For example two or more blocks shown in succession in Figs. 3 and 4 may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved.

Substitute the section heading on page 17, line 1, with the following:

A14 ~~CLAIMS~~ CLAIMS

Substitute the section heading on page 22, line 1, with the following:

A15 ~~ABSTRACT~~ ABSTRACT